This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1.-23. (cancelled)

24. (currently amended) A method of password generation comprising ~~the steps of~~:

providing a biometric information sample;

determining from the sample a first string including a plurality of symbols, the symbols based on features within the biometric information sample;

determining a plurality of strings in dependence upon predetermined characteristics in relation to the first string;

hashing the strings from the determined plurality of strings to produce a plurality of hash values; and

comparing each hash value from the plurality of hash values against a stored hash value determined during an enrollment process for determining at least one hash string from the plurality of hash strings indicative of a match,

wherein upon a match between a hash value from the plurality of hash values and the stored hash value, the string from the plurality of strings and associated with the matching hash value is provided as the generated password.

25.-27. (cancelled)

28.(original) A method of password generation according to claim 24 wherein the first string is ordered based upon its symbol content.

29. (original) A method of password generation according to claim 28 wherein the strings

from the plurality of strings are ordered based upon their symbol content.

30. (currently amended) A method of password generation according to claim 24 wherein ~~the step of~~ determining a plurality of strings in dependence upon predetermined characteristics comprises ~~the steps of~~:

capturing an image of a biometric information sample from a biometric information source;

extracting a number r of features from the biometric information sample and encoding r symbols, one per feature; and,

extracting a number δ of extra features, and encoding δ extra symbols, one per extra feature, and

wherein ~~the step of~~ comparing the string includes ~~the step of~~ determining a number of symbols within the string that are absent from the previously stored string and deleting those symbols.

31. (original) A method of password generation according to claim 24 wherein upon the comparison of each hash value from the plurality of hash values against a stored hash value determined during an enrollment process is indicative of other than at least one hash string from the plurality of hash strings matches, verifying if the plurality of hash strings includes all the hash strings that can be generated within predetermined characteristics.

32. (original) A method of password generation according to claim 24 wherein the generated password is an unordered generated password.

33. (currently amended) A method of password generation according to claim 25 wherein ~~the step of~~ encoding symbols is performed in dependence upon extracted feature type.

34. (original) A method of password generation according to claim 24 wherein a symbol

is encoded as an n-bit value.

35. (currently amended) A method of password generation comprising ~~the steps of~~:

providing a biometric information sample from an individual;

determining a location of an alignment feature within the biometric information sample;

extracting features from the biometric information sample;

determining from the extracted features a first string of symbols based on locations of extracted features within the biometric information sample relative to the alignment feature;

determining a plurality of error strings in dependence upon predetermined parameters defining an error region about the extracted first string;

hashing the first string and at least some of the error strings from the determined plurality of strings to produce a plurality of hash values; and

comparing each produced hash value from the plurality of hash values with a predetermined stored hash value for determining a hash value from the plurality of hash values indicative of a match,

wherein upon a match between a hash value from the plurality of hash values and the stored hash value, the string from which the matching hash value was derived is provided as the generated password.

36. (currently amended) A method of password generation according to claim 35 comprising ~~the step of~~: providing an indication of the first feature.

37. (currently amended) A method of password generation according to claim 36 wherein ~~the step of~~ providing an indication of the first feature includes ~~the step of~~ selecting the first feature from a plurality of potential first features.

38. (currently amended) A method of password generation according to claim 36 wherein ~~the step of~~ providing an indication of the first feature includes ~~the step of~~ selecting

a region within the biometric information sample, the region being indicative of the first feature from a plurality of potential first features.

39. (new) A method of generating biometric data comprising:

receiving a first set of data from a biometric input device, the first set of data derived from a biometric sample;

identifying data from the first set of data corresponding to a first feature of the biometric sample in accordance with a first predetermined algorithm;

analysing the first set of data to determine features therein and to determine at least a parameter associated with the features and for providing a plurality of overlapping subsets of the features, at least some of the overlapping subsets including fewer than all of the features within the set of data.

40. (new) A method of generating biometric data according to claim 39 wherein the parameter associated with the features comprises data relating to a feature type.

41. (new) A method of generating biometric data according to claim 40 wherein the parameter associated with the features comprises data indicative of a position of the feature relative to the first feature.

42. (new) A method of generating biometric data according to claim 41 comprising hashing data corresponding to the plurality of overlapping subsets of the features.

43. (new) A method of generating biometric data according to claim 42 wherein the hashing comprises using a hashing algorithm that is insensitive to the order of the data provided thereto.

44. (new) A method of generating biometric data according to claim 39 wherein the parameter associated with the features comprises data indicative of a position of the feature relative to the first feature.

45. (new) A method of generating biometric data according to claim 44 comprising:

hashing data associated with the at least a parameter using a hashing algorithm to generate a hash value.

46. (new) A method of generating biometric data according to claim 44 comprising:

hashing data associated with the at least a parameter using a hashing algorithm to generate a plurality of hash values, each of the hash values corresponding to a specific overlapping subset of the features.

47. (new) A method of generating biometric data according to claim 46 wherein the hashing comprises using a hashing algorithm that is insensitive to the order of the data provided thereto.

48. (new) A method of generating biometric data according to claim 47 comprising:

receiving a set of user data from a second biometric input device, the set of user data derived from a biometric sample of a user;

identifying user data from the set of user data corresponding to a first user feature of the user biometric sample in accordance with the first predetermined algorithm;

analysing the user data to determine user features therein and to determine at least a user parameter associated with the user features and for providing a plurality of overlapping subsets of the user features, at least some of the overlapping subsets including fewer than all of the user features within the set of user data;

hashing user data associated with the at least a parameter using a hashing algorithm to generate a user hash value; and,

comparing the user hash value with the plurality of hash values to determine if the biometric sample of the user corresponds to the biometric sample.